Baba Ghulam Shah Badshah University Rajouri (J&K)

(SYNOPSIS FOR REGISTRATION FOR DEGREE OF DOCTOR OF PHILOSPHY IN COMPUTER SCIENCE)

Proposed Topic	:	**Analyzing & Interpreting the Threat Mitigation Strategies in Information Systems: Conceptual and Operational Explorations**
Name of the Candidate	:	Mr. Qamar Rayees Khan
Name of the Supervisor	:	**Supervisor:** Prof. M. Asger Department of Computer Sciences, BGSB University Rajouri. **Co-Supervior:**
School/Department	:	Computer Sciences
Date of Re-Submission	:	12/03/2012

Signature of the Candidate

Signature of the Supervisor

Analyzing & Interpreting the Threat Mitigation strategies in Information Systems: Conceptual and Operational Explorations

Background

Information security means protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction.[12] The term "information security" has many definitions. Depending upon one's viewpoint, it can be technical, behavioral, managerial, philosophical, and/or organizational. Von Solms [2006] characterizes information security in waves, progressing from technical to managerial [2]. According to Anderson it is "A well-informed sense of assurance that information risks and controls are in balance"[13].The terms information security, computer security and information assurance are frequently used interchangeably. These fields are interrelated and share the common goals of protecting the confidentiality, integrity and availability of information. Information security is concerned with the confidentiality, integrity and availability of data regardless of the form the data may take: electronic, print, or other forms [10].**Confidentiality** is the term used to prevent the disclosure of information to unauthorized individuals or systems. **Integrity** means that data cannot be modified undetectably. For any information system to serve its purpose, the information must be **available** when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. Should confidential information fall into the hands of a competitor, such a breach of security could lead to excessive loss. These Information Security approaches also pave a new way towards implementation of effective data mining procedures for data protection, security and privacy. That is, how to ensure the user's privacy while their data are being mined. Researchers have also stated that if we do not solve the privacy issue, data mining will become a derogatory term to the general public.

Literature Survey

The field of information security has grown and evolved significantly in recent years. The end of the 20th century and early years of the 21st century saw rapid advancements in telecommunications, computing hardware and software. The availability of smaller, more powerful and less expensive computing equipment made electronic data processing within the reach of small business and the

home user. These computers quickly became interconnected through a network generically called the Internet or World Wide Web.

The rapid growth and widespread use of electronic data processing and electronic business conducted through the Internet, along with numerous occurrences of international terrorism, fueled the need for better methods of protecting the computers and the information they store, process and transmit as defined by CNSS [3]. The academic disciplines of information security and information assurance emerged along with numerous professional organizations - all sharing the common goals of ensuring the security and reliability of information systems. Security of information resources must include controls and safeguards to offset possible threats as well as controls to ensure timeliness, availability, integrity, confidentiality, etc. [9].

Being one of the most fundamental security properties, integrity is subject to a vast area of research. We refer to security textbooks [41, 42] that discuss assorted flavors of integrity, and integrity surveys [43, 44] and tutorials [45] that develop integrity classifications. To the best of our knowledge, our framework is the first to unify information integrity for programs. As mentioned previously, our departure point is the classification by Li et al. [46]. Our contribution compared to this classification is a more general model of invariants (Li et al. only discuss predicate invariants), a more general model of information flow (Li et al. do not consider endorsement), and a unified view, where we show that program correctness subsumes invariance policies. In addition, we also offer a unified enforcement mechanism that guarantees all aspects of integrity at once. Information-flow integrity dates back to Biba's integrity model [47], which dualizes Bell and LaPadula's model [48, 49] for mandatory access control. The Clark-Wilson integrity model [50] is a classical model that focuses on separation of duties and transactions.

Although information integrity for programs has been unexplored compared to confidentiality, it has recently received increasing attention. Languages such as Perl, PHP, and Ruby offer dynamic integrity checks that are based on tainting, a runtime mechanism for tracking explicit flows. Ørbæk and Palsberg [51, 52] define instrumented information-flow semantics for integrity in λ-calculus. The semantics is based on integrity label manipulation. An unsoundness related to the impact of flow sensitivity on information flow has been recently uncovered. Heintze and Riecke [53] consider integrity as dual to confidentiality in their study of information flow for a language based on λ-calculus. Li and Zdancewic unify confidentiality and integrity policies [54] in the context of

information downgrading. A line of work on robust declassification [55, 56, 57] is based on an interplay between confidentiality and integrity, where information release (of high confidentiality data) is allowed only if it cannot be manipulated by the attacker (through attacker-controlled low integrity data) to release additional information. The Java-based Jif tool [36], as well as its web-based extensions [58, 59], implement robustness policies.

Sabelfeld and Sands [60] introduce dimensions of declassification, with the main focus on declassification of confidentiality levels. They informally discuss the dual of dimensions of declassification: dimensions of endorsement. We draw on delimited release [53] when it comes to enforcement of integrity policies. Although delimited release is a confidentiality property, its enforcement includes information-flow aspects and is capable of enforcing generalized invariants. This paper builds on a runtime mechanism for delimited release by Askarov and Sabelfeld [54]. A static alternative to tracking delimited release has been explored by Sabelfeld and Myers [53]. Boudol and Kolundzija [61] combine programming constructs for expressing access control and declassification policies. Access control is represented at language level, with explicit granting, restricting, and testing access rights. Information-flow policies and access control have been also integrated at language level by Banerjee and Naumann [62], although without considering declassification.

Bhavani [68] proposed the use of data mining to preserve the privacy of information. He also examined data mining applications in security and their implication for privacy. Upadhayay [69] addresses the privacy issues in data mining and developed a novel privacy preserving data mining technique.

Haack et al. [63] explore reasoning about explicit flows in program logic. They arrive at two kinds of integrity notions: flow-based and format-based. The former is an information-flow policy, and the latter is concerned with proper formatting (they give an example policy such as “a phone number field should only contain numbers”). This latter type of integrity is subsumed by generalized invariance. Cheney et al. [64] investigate semantic foundations for data provenance in databases. Provenance is concerned with tracking the origin of information, and so Cheney et al. model it as a dependency analysis. Diserholt [65] proposes a library that handles confidentiality and integrity policies in Haskell. Besides handling confidentiality, the library is also able to combine information-flow integrity,

predicate invariants, and some means for access control. Similarly to this paper, their work is inspired by the classification of integrity policies in [66].

Clarkson and Schneider [67] propose contamination and suppression as quantitative definitions of integrity. The former is dual to quantitative information leakage, whereas the later measures how much information is lost from outputs. The study of suppression includes program suppression due to malicious influence and implementation errors as well as channel suppression due to information loss about inputs to a noisy channel.

A threat is anything (man made or act of nature) that has the potential to cause harm. The likelihood that a threat will use a vulnerability to cause harm creates a risk. When a threat does use a vulnerability to inflict harm, it has an impact. In the context of information security, the impact is a loss of availability, integrity, and confidentiality, and possibly other losses [10]. While access-control mechanisms, firewalls and so forth may help counter such losses, we can never be confident about security unless we are provided with some assurance of their effectiveness. Such assurance may be achieved, in part, by analyzing whether a formal description of the system upholds certain security properties. These properties include confidentiality (no unauthorized release of information) and integrity (no unauthorized modification of information).

The study of integrity [23][25] as a formal security property has received little attention within the research community; confidentiality has been extensively studied and is the better understood of the two properties[29]. Information security has become one of the most important issues of any information systems. Thus, the information systems needs to ensure that their information assets are properly protected and maintains high level of information security. An acceptable level of information security can only be introduced and maintained if the correct set of security controls, both procedural and technical, are identified, implemented and maintained (Solms R. 1998). The first step in creating a secure information system is to identify threats. Once potential problems are known, the second step, establishing controls, can be taken. Finally, the third step consists of audits to discover any breach of security [11]. According to Kankanhalli et al. [5], preventive efforts include deploying advanced security software or controls to protect IS assets, such as advanced access control, intrusion detection, firewall, surveillance mechanisms, and the generation of exception reports. As proposed by von Solms et al. [9], the security baseline should trace all countermeasures for all IS assets and threats.

The 2001 Computer Crime and Security Survey [7] reported that 196 of the respondents to the survey could quantify their losses due to unauthorized use of computer systems at a total of US$378 million in the previous year. While access-control mechanisms, firewalls and so forth may help counter such losses, we can never be confident about security unless we are provided with some assurance of their effectiveness. The CSI/FBI 2005 [4] security survey reports 13 different attack types, ranging from website defacement to financial fraud to Internet worms and viruses. There are several reports in the business press that point to the increasing number of vulnerabilities in commonly used software as well as viruses and other threats that seek to exploit these vulnerabilities, and detail how it is becoming an increasing problem for any Information system.

Effective counter measures sometimes exist for many of these threats, but are often not correctly deployed due to the specific characteristics of the information systems in use, or the capabilities of the IT staff. The type of Security countermeasures adopted and their implementation did not necessarily affect the threat perception of the Information System. Analyses of responses suggested that the scope of the countermeasures adopted were not adequate with the severity of the perceived threats [1]. A security countermeasure refers to a way to detects, prevent, or minimize losses associated with a specific IS threat [8]. Whitman [6] listed various leading IS threats that target the Information systems.

2. Justification of the proposed work.

Errors in computerized information systems were relatively manageable as long as there was homogenous system environment and centralized control over information.

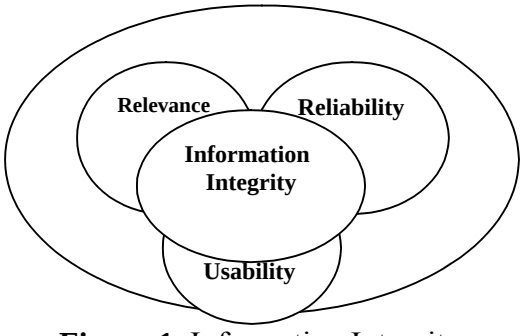

Figure 1. Information Integrity

According to the ITGI (2004), the external oval in Figure 1 encompasses information and the three circles within the oval illustrate attributes of information quality [26][27]. The attribute, which is the central oval, represents information integrity. The strategic placement of this oval illustrates the significance of integrity to the information's value. As mentioned, it is important to observe the

positioning of the information integrity oval in relation to the three circles (relevance, usability and reliability), thereby overlapping and incorporating the elements of all three. Applied to information, 'integrity is the representational faithfulness of the information to the condition or subject matter being represented by the information'. Emerging trends of globalization, changing organizational patterns, strategic partnering, and electronic commerce and distributed computing have changed all this, resulting in loss of integrity in information systems[15][16]. These errors are essentially caused by online factors of change, complexity, communication, conversion and corruption (the 5 C's). These factors have their presence in IS mainly through system environment that is external to computing (and hence the application) system and overlaps the user environment. In spite of application controls, it is these external factors that then introduce in information systems, errors that are made but not corrected [15][16]. It is within above framework of errors in computerized information systems and their integrity implications, that research investigations presented at IFIP TC 11 WG 11.5 Second Working Conference [Mandke and Nayar, 1998] identify intrinsic integrity attributes[22] of accuracy[28], consistency and reliability which, irrespective of nature of use, any IS must satisfy. Research investigations further observe that depending on the context and nature of use there can be other optional integrity attributes of security and privacy that can be seen as extrinsic or subjective integrity attributes specific to area of use [Mandke, 1996][14]. Other such subjective attributes of integrity could be: interpretability, understandability, tractability, flexibility, etc. [Wang and Strong, 1993]. It is to ensure above integrity attributes that research investigations presented at IFIP TC 11 WG 11.5 Second Working Conference [17] have proposed need to incorporate online learning and error correcting mechanisms in the IS models[17][18]. Specifically, to account for errors in IS that are made but not corrected, they propose incorporation of automatic feedback control systems with error detection and correcting technologies for improved information [26][27][28] accuracy, consistency and reliability; technologies that maximize integrity of information systems - Information Integrity Technologies[17][19]. They further argue that, when incorporated, it is such Information Integrity Technology that would also facilitate demonstrating improved integrity of information obtained, rather than merely trusting the computerized information systems [20]. There are obvious difficulties in implementing such automatic feedback control systems, the most important being to study error patterns. Specifically, it is not possible to track and analyze every bit of data/information for all times as it flows through the information system stages. Way out here is to consider Information Integrity Technology that takes a sample of input data at the output or at an intermediate point of an appropriately identified stage or subsystem of the IS and then follows or keeps track of the sampled

records at output or intermediate points of subsequent stages (subsystems), at a given point of time or at different points of time over a required time interval [16][17].

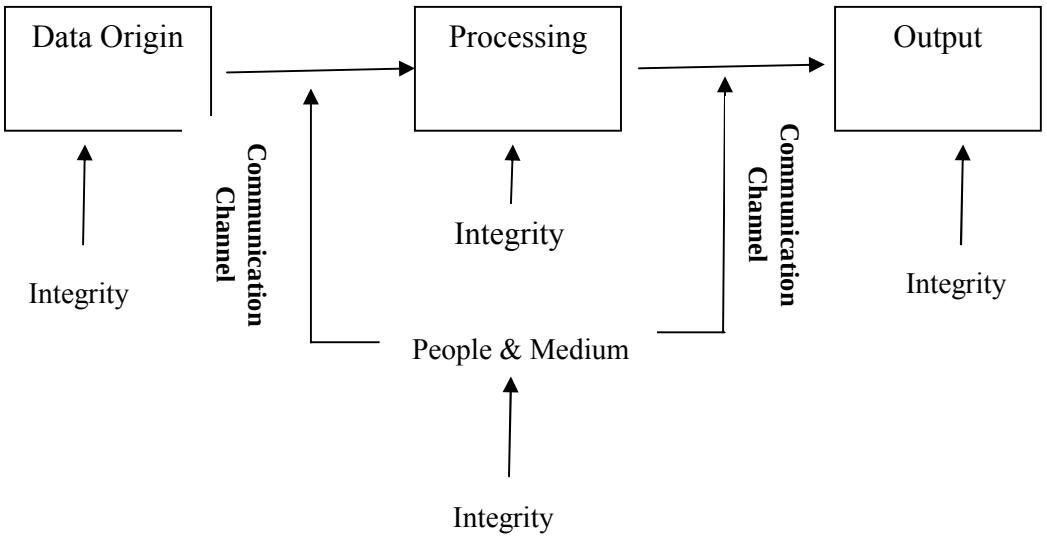

Figure 2. Conceptual Presentation of Integrity of an Information System.

3. Objectives

The Objective of this research is to improve the optimum Integrity in Information System by quantifying intrinsic integrity attributes of accuracy, consistency and reliability on the data to be mined. It has been observed that after applying such attributes the data may get modified from its original version. So as to apply counter measure, a comparative analysis could also be carried out on the data before and after evaluation of such attributes so that effective measures are taken to not only evaluate the knowledge integrity of the data but also the measures to evaluate the knowledge integrity of individual patters.

4. Material proposed to be used for the investigation

There exists a wide variety of data mining tools with commercial and open-source licenses. This is particularly true in the business application user group, where commercial software is very attractive due to high software stability, good coupling with other commercial tools for data warehouses, included software maintenance, and the possibility of user training for sophisticated topics.

Data mining suites (DMS) /Tools focus largely on data mining and include numerous methods. They support feature tables and time series, while additional tools for text mining are sometime available. The application focus is wide and not restricted to a special application field, such as business applications; however, coupling to business solutions, import and export of models, reporting, and a variety of different platforms are nonetheless supported. In addition, the producers provided services for adaptation of the tools to the workflows and data structures of the customer.

DMS is mostly commercial and rather expensive, but some open-source tools such as RapidMiner exist. The major data mining tools which could be used in the proposed research for pattern matching and normal data distribution from heterogeneous data sources include IBM SPSS Modeler, SAS Enterprise Miner, Alice d'Isoft, DataEngine, DataDetective, GhostMiner, Knowledge Studio, KXEN, NAG Data Mining Components, Partek Discovery Suite, STATISTICA, and TIBCO Spotfire. In addition to above mentioned tools for data mining the following supporting tools are also required.

a) Machine (PC: Latest Configuration)
b) Database System using Oracle 9i or higher, SQL Server 2005 or higher
c) Subscription to IEEE
d) Front End Packages.

5. Methodology proposed to be followed

Within the framework of Information Integrity attributes of Accuracy (A), Consistency (C) and Reliability (R) argued, we can then identify Information Integrity Technology Implementation steps as follows:

i. Understand the user application of the computerized information system under consideration and Establish organizational standard pertaining to data/information vis-à-vis requirements of: accuracy, consistency, reliability and cumulative integrity, based on application area and study of organizational practices.
ii. Study data/information flow through the Information System and define source and destination data sources.

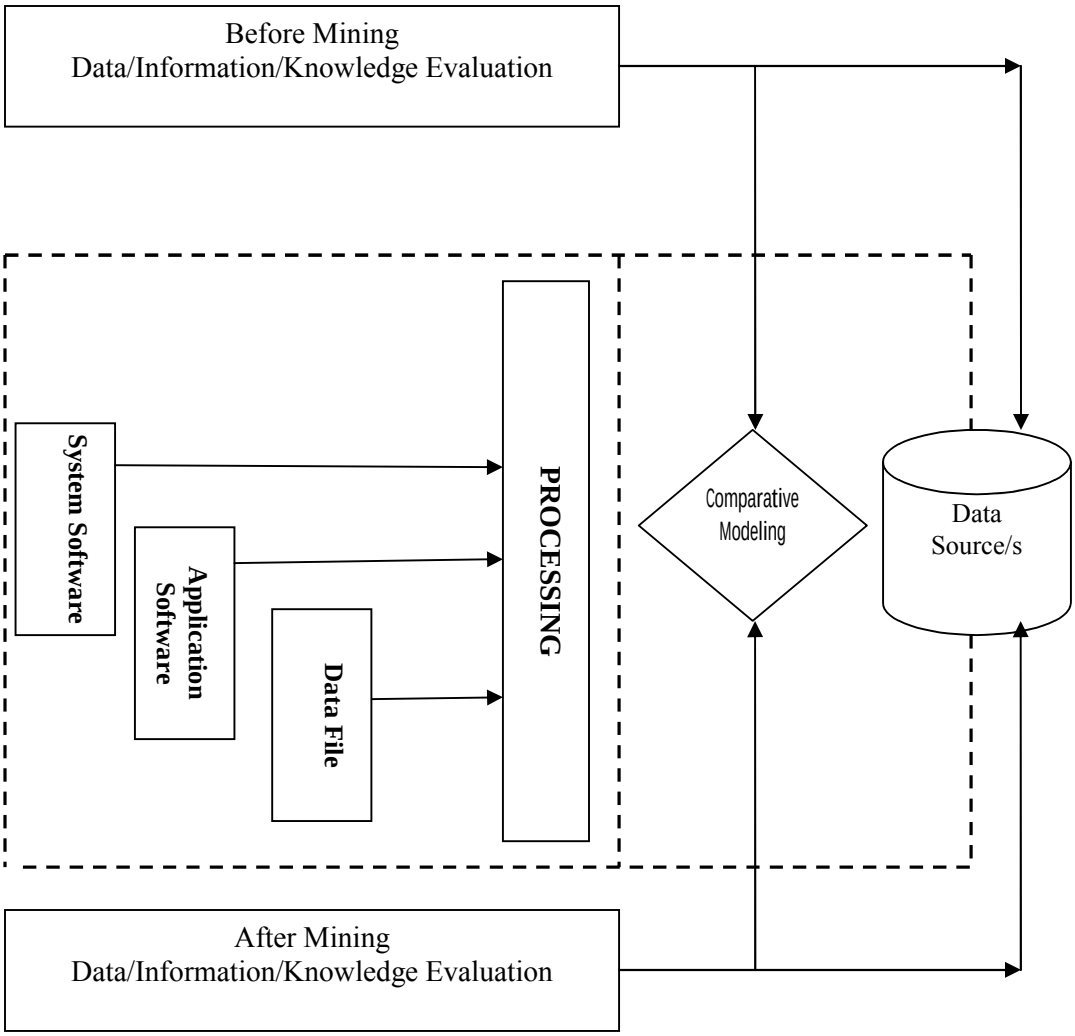

Figure 3. Data/Information Flow Model for an Information System for Implementing Information Integrity Technology

iii. Develop the Information System Model as in Figure (3), based on understanding of data/ information flow in the system for the identified data sources and Specify and document data rules, also known as edits, to be implemented to study accuracy and consistency of the data/information in proposed system.

iv. Choose a method for calculating Reliability Index, keeping in view advantages, disadvantages and convenience of application while accounting for factors such as nature of available data, form of data and available computation aids.

v. Propose Integrity Analysis method for analyzing intrinsic Integrity attributes of accuracy, consistency and reliability. In addition, the proposed method may also undertake statistical analysis (time series analysis and other techniques) of error patterns signifying irregular changes, which contributes to loss of accuracy and consistency and of causes, which contribute to loss of Reliability.

vi. The proposed method can be modified for analyzing the error Detection Database constructs so as to identify data rule violations in respect of accuracy and consistency attributes and establish degree of integrity of data/ information in respect of Information Integrity.

vii. Perform Comparative study of the Integrity profile and indices obtained with: standards in local, regional, national, international as the case may be – and the user specification on Integrity, so as to know what is expected of Information Integrity Technology. This would also facilitate ordering or ranking of the Integraty attributes from the points of which attributes needs maximum improvement effort. This can also provide efficiencies and deficiencies for proposed system and will also pave way to propose certain modification on the proposed system so that these deficiencies are minimized.

viii. After locating the pairs of a give field at a given subsystem, each for improvements of accuracy and consistency and having located given subsystems for reliability improvement opportunities, further analyze the Error Detection Database and study irregular changes at each of pairs corresponding to accuracy and consistency attributes and study reliability factors at each of the subsystems, so as to understand over the time error patterns and causesd contributing to loss of accuracy, consistency and reliability. This would then facilitate detection of error orcause the occurred sometime in the past or estimating error or cause at time (t), or predict error or cause that may occur in feature.

ix. Also propose a Comparative Study performance of the Information System on incorporation of the Information Integrity Technology as discussed in the research on other data sources. Accourdingly obtained the intrinsic Information Integrity attribute indices, Integrity profile and Cumulative Informatiobn Integraty Index and compare them with appropriate reports before implementation of information Integrity Technology available.

x. Finally after applying various attributes on various Information Systems/ Data Sources the proposed system is evaluated for whether these intrinsic attributes have modified the data from its original version or not. These changes could be detrimental for the data and need to be analyzed properly. To overcome these situations effective data mining techniques will be

implemented before and after these operations are carried on the proposed data like Classification, Clustering, Association, Predication and Sequential Patterns.

6. Possible outcome of the investigation

The possible outcome of the work would be an improved Integrity in Information System by quantifying intrinsic integrity attributes of accuracy, consistency and reliability. The proposed work will also provide a comparative study, that before and after applying intrinsic integrity attributes whether the data is or is not modified from its original version. This is evaluated using some existing data mining techniques before and after on the proposed data and analyzing the change in data. Methods shall be implemented to ensure that the change in data is minimal and the data is secure.

Bibliography

[1] Quey-Jen Yeh , Arthur Jung-Ting Chang Threats and countermeasures for Information system Security: A cross-industry study, Elsevier, 2007.

[2] von Solms, B. (2006). "Information Security: The Fourth Wave," Computers & Security (25) 3, pp. 165-168.

[3] CNSS, National Information Assurance (IA) Glossary (CNSS Instruction No. 4009), Committee on National Security Systems, revised in June 2006.

[4] Lawrence A. Gordon, Martin P. Loeb, and William Lucyshyn. 2005 csi/fbi computer crime and security survey, 2005.

[5] Kankanhalli, H.H. Teo, B.C.Y. Tan, K.K. Wei, An integrative study of information systems security effectiveness, International Journal of Information Management 23, 2003, pp. 139–154.

[6] M.E. Whitman, Enemy at the gates: threats to information security, Communication of the ACM 46 (8), 2003, pp. 91–95.

[7] Lawrence A. Gordon and Martin P. Loeb. The economics of information security investment. ACM Trans. Inf. Syst. Secur., 5(4):438–457, 2002.

[8] T.R. Peltier, Information Security Risk Analysis, Auerbach, New York, 2001.

[9] R. von Solms, H. van de Haar, S.H. von Solms, W.J. Caelli, A framework for information security evaluation, Information and Management 26 (3), 1994, pp. 143– 153.

[10] K.D. Loch, H.H. Carr, M.E. Warkentin, Threats to information systems: today's reality, yesterday's understanding, MIS Quarterly 16 (2), 1992, pp. 173–186.

[11] K.J.Kanapp, Thomas E. Marshall, R. Kelly, Dorsey W. Morrow-International Information systems security, ISC Survey.

[12] Gurpreet Dhillon, Challenges in Managing Information Security in the New Millennium Gurpreet Dhillon College of Business, University of Nevada, Las Vegas.

[13] Anderson, J. M. (2003). "Why We Need a New Definition of Information Security," Computers & Security (22)4, pp.308-313.
[14] Delone M. H., and McLean E. R. (1992) Information Systems Success: The Quest for the Dependent Variable,Information Systems Research 3 (1).
[15] Mandke Vijay V. (1996) Research in Information Integrity: A Survey and Analysis, Proceedings of the JNCASR and SERC Discussion Meeting at IISc Campus, Bangalore on Information integrity --Issues and Approaches, Edited by Rajaraman V. and Mandke Vijay V., published by Information Integrity Foundation, New Delhi, India.
[16] Mandke Vijay V., and Nayar M.K. (1997) Information Integrity --A Structure for its Definition, Proceedings of the 1997 Conference on Information Quality, Edited by Diane M. Strong and Beverly K. Kahn, MIT, Cambridge, Massachusetts, USA.
[17] Mandke Vijay V., and Nayar M.K. (1998) Design Basis for Achieving Information Integrity—A Feedback Control System Approach, IFIP TC 11 Working Group 121.5 Second Working Conference on Integrity and Internal Control in Information Systems, Edited by Sushil Jajodia, William List, Graeme W. McGregor and Leon A.M. Strous, Published by Kluwer Academic Publishers.
[18] Mandke Vijay V., and Nayar M.K. (1999) Modeling Information Flow for Integrity Analysis, Proceedings of the 1999 Conference on Information Quality, Edited by Y. V. Lee and G. K. Tayi, MIT, Cambridge, Massachusetts, USA.
[19] Mandke Vijay V., and Nayar M.K. (2001) Information Envelope and its Information Integrity Implications: For a complex, changing environment,modeling a Generic business process as an integral to a closed loop information and control System characterized by uncertainty, proceedings of the 2001 Conference on Information Quality, Edited by Elizabeth M. Pierce and Raissa KatzHass, MIT, Cambridge, Massachusetts, USA.
[20] Rajaraman V. (1996) Information Integrity --An Overview, Proceedings of the JNCASR and SERC Discussion Meeting at IISc Campus, Bangalore on Information Integrity --Issues and Approaches, Edited by Rajaraman V., and Mandke Vijay V., published by Information integrity Foundation, New Delhi, India.
[21] Tallberg Anders (1999) An Economic Framework For Information Integrity, Forskning srapporter Research Reports, Swedish School of Economics and Business Administration.
[22] Wang R. and Strong D. (1993) An empirical Investigation of Data Quality Dimensions: A Data Consumer' s Perspective, TDQM9312, The TDQM Research Program, MIT, Sloan School of Management, Cambridge, USA.
[23] K.J. Biba. Integrity considerations for secure computer systems. Technical Report MTR-3153 Rev 1 (ESD-TR-76-372), MITRE Corp Bedford MA, 1976.
[24] J.L. Jacob. The basic integrity theorem. In Proceedings of the Computer Security Foundations Workshop IV, pages 89–97. IEEE Computer Society Press, June 1991.
[25] Boritz, J.E. 2005. IS practitioners' views on core concepts of information integrity. International Journal of Accounting Information Systems 6:260-279.
[26] Bovee, M.W. 2004. Information quality: a conceptual framework and empirical validation. [Online]. Available WWW:http://www.bsad.uvm.edu/Research/FacPubs/details?author=265 (Accessed 9 December 2005).
[27] Bovee, M., Srivastava, R.P. and Mak, B. 2003. A conceptual framework and belief-function approach to assessing overall information quality. International Journal of Intelligent Systems 18(1):51-74.

[28] Wang, R.Y. and Strong, D.M. 1996. Beyond accuracy, what data quality means to data consumers. Journal of Management Information Systems 12(4):5-34.
[29] S. Flowerday and R. von Solms . What constitutes information integrity? Vol.9(4) December 2007 – A Review Article
[30] Wang R. and Strong D. (1993) An empirical Investigation of Data Quality Dimensions: A Data Consumer' s Perspective, TDQM9312, The TDQM Research Program, MIT, Sloan School of Management, Cambridge, USA.
[31] Agmon, N., and Ahituv, N., Assessing Data Reliability in an Information System, Journal of MIS, 4(2), 34-44, 1987
[32] Morey, R.C., Estimating and Improving the Quality of Information in the MIS, Communications of the ACM, 25(5), 337-342, 1982
[33] Baker, H.B., Information Integrity-Structure for its Definition and Management, McGraw Hill Book Company, NY – 1983.
[34] Hansen, M.D., and Wang, Y.R., Managing Data Quality : A Critical Issue for the Decade to Come, Working Paper, Alfred P.Sloan School of Management, MIT,USA, March, 1991
[35] W. Shockley. Implementing the clark/wilson integrity policy using current technology. In Proceedings of NIST-NCSC National Computer Security Conference, pages 29–37, 1998.
[36] Wang, R. et al., 1995. Toward Quality Data: An Attribute-Based Approach. Decision Support Systems, Vol. 13, 1995. 25jang, Y. et al., 1995. A Qualitative Approach to Automatic Data Quality Judgement. Journal of Organizational Computing, 5 (2) 1995.
[37] Spencer, B., 1985. Optimal Data Quality. Journal of the American Statistical Association, Vol. 80, 1985.
[38] List, W. and Melville, R., 1994. Integrity in Information Systems, IFIP WG 11.5, June 1994.
[39] Fox, C. et al., 1994. The Notion of Data and its Quality Dimensions. Information Processing and Management, 30 (1) 1994.
[40] ITGI. 2004. Managing enterprise information integrity: security, control and audit issues. USA: IT Governance Institute.
[41] C. P. Pfleeger and S. L. Pfleeger. Security in Computing (4th Edition). Prentice Hall, 2006.
[42] D. Gollmann. Computer Security (2nd Edition). Wiley, 2006.
[43] T. Mayfield, J. E. Roskos, S. R. Welke, J. M. Boone, and C. W. McDonald. Integrity in automated information systems. Technical Report P-2316, Institute for Defense Analyses, 1991.
[44] R. S. Sandhu. On five definitions of data integrity. In Proceedings of the IFIP WG11.3 Working Conference on J. Guttman. Invited tutorial: Integrity. Presentation at the Dagstuhl Seminar on Mobility, Ubiquity and Security, Feb. 2007. http://www.dagstuhl.de/07091/. Slides at http://web.cs.wpi.edu/˜guttman/.
[45] C. Dima, C. Enea, and R. Gramatovici. Nondeterministic nointerference and deducible information flow. Technical Report 2006-01, University of Paris 12, LACL, 2006.
[46] K. J. Biba. Integrity considerations for secure computer systems. Technical Report ESDTR-76-372, USAF Electronic Systems Division, Bedford, MA, Apr. 1977. (Also available through National Technical Information Service, Springfield Va., NTIS AD-A039324.).
[47] D. E. Bell and L. J. LaPadula. Secure computer systems: Mathematical foundations. Technical Report MTR-2547, Vol. 1, MITRE Corp., Bedford, MA, 1973.
[48] L. J. LaPadula and D. E. Bell. Secure computer systems: A mathematical model. Technical Report MTR-2547, Vol. 2, MITRE Corp., Bedford, MA, 1973. Reprinted in J. of Computer Security, vol. 4, no. 2–3, pp. 239–263, 1996.

[49] D. D. Clark and D. R.Wilson. A comparison of commercial and military computer security policies. In Proc. IEEE Symp. on Security and Privacy, pages 184–193, May 1987. [38] P. Ørbæk. Can you trust your data? In Proc. TAPSOFT/FASE'95, volume 915 of LNCS, pages 575–590. Springer-Verlag, May 1995.
[50] P. Ørbæk and J. Palsberg. Trust in the λ-calculus. J. Functional Programming, 7(6):557– 591, 1997.
[51] N. Heintze and J. G. Riecke. The SLam calculus: programming with secrecy and integrity. In Proc. ACM Symp. on Principles of Programming Languages, pages 365–377, Jan. 1998.
[52] P. Li and S. Zdancewic. Unifying confidentiality and integrity in downgrading policies. In Workshop on Foundations of Computer Security, pages 45–54, June 2005.
[53] S. Zdancewic and A. C. Myers. Robust declassification. In Proc. IEEE Computer Security Foundations Workshop, pages 15–23, June 2001.
[54] A. C. Myers, A. Sabelfeld, and S. Zdancewic. Enforcing robust declassification and qualified robustness. J. Computer Security, 14(2):157–196, May 2006.
[55] A. Askarov and A. C. Myers. A semantic framework for declassification and endorsement. In Proc. European Symp. on Programming, LNCS, Mar. 2010.
[56] A. C. Myers, L. Zheng, S. Zdancewic, S. Chong, and N. Nystrom. Jif: Java information flow. Software release. Located at http://www.cs.cornell.edu/jif, July 2001.
[57] S. Chong, K. Vikram, and A. C. Myers. Sif: Enforcing confidentiality and integrity in web applications. In Proc. USENIX Security Symposium, pages 1–16, Aug. 2007.
[58] S. Chong, J. Liu, A. C. Myers, X. Qi, K. Vikram, L. Zheng, and X. Zheng. Secure web applications via automatic partitioning. In Proc. ACM Symp. on Operating System Principles, pages 31–44, Oct. 2007.
[59] A. Sabelfeld and D. Sands. Declassification: Dimensions and principles. J. Computer Security, 17(5):517–548, Jan. 2009.
[60] A. Sabelfeld and A. C. Myers. A model for delimited information release. In Proc. International Symp. on Software Security (ISSS'03), volume 3233 of LNCS, pages 174–191. Springer-Verlag, Oct. 2004.
[61] A. Askarov and A. Sabelfeld. Tight enforcement of information-release policies for dynamic languages. In Proc. IEEE Computer Security Foundations Symposium, July 2009.
[62] G. Boudol and M. Kolundzija. Access-control and declassification. In Proc. Mathematical Methods, Models, and Architectures for Computer Networks Security, volume 1 of Communications in Computer and Information Science, pages 85–98. Springer-Verlag, Sept. 2007.
[63] A. Banerjee and D. A. Naumann. Stack-based access control and secure information flow.Journal of Functional Programming, 15(2):131–177, Mar. 2005.
[64] C. Haack, E. Poll, and A. Schubert. Explicit information flow properties in JML. In Proc. WISSEC, 2008.
[65] J. Cheney, A. Ahmed, and U. Acar. Provenance as dependency analysis. In Proc. Database Programming Languages, 2007.
[66] A. Diserholt. Providing integrity policies as a library in Haskell. Master Thesis, Chalmers University of Technology, Gothenburg, Mar. 2010. http://www.cse.chalmers.se/ ˜russo/albert.htm.
[67] M. Clarkson and F. B. Schneider. Quantification of integrity. In Proc. IEEE Computer Security Foundations Symposium, July 2010.
[68] Bhavani Thuraisingham. Data mining for security Applications and Its privacy implications.Springer, 2009.

[69] A.K.Upadhayay, Abhijat Agarwal, Rachita Masand and Rajeev Gupta. Privacy Preserving Dara Mining: A New Methodology for Data Transformation, Proceedings of the first International Conference on Intelligent Human Computer Interaction,2009.